UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,687	12/22/2000	Xun Wilson Huang	21816-04953	4655

758 7590 04/18/2006

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
ZHEN, LI B	
ART UNIT	**PAPER NUMBER**
2194	

DATE MAILED: 04/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/747,687	HUANG ET AL.	
	Examiner	Art Unit	
	Li B. Zhen	2194	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,16-32,36-52 and 56-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,16-32,36-52 and 56-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

WILLIAM THOMSON
SUPERVISORY PATENT EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date IDS 2/3/06
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12,16-32,36-52 and 56-58 are pending in the application.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 02/03/2006 has been entered.

Response to Arguments

3. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-12, 16, 18, 21-32, 36, 38, 41-52, 56 and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,496,847 Bugnion et al. [hereinafter referred to as Bugnion] in view of U.S. Patent No. 6,785,728 to Schneider et al. [hereinafter referred to as Schneider].**

6. As to claim 1, Bugnion teaches the invention substantially as claimed including a computer-implemented method for virtualizing user privileges in a computer operating system [computer is operationally divided into a system level and a user level and the

computer accepts and carries out a pre-determined set of privileged instruction calls only from sub-systems at the system level; col. 4, lines 40-52] including multiple virtual private servers [virtual operating system (VOS) 370, 372, Fig. 3; col. 8, lines 5-20], the method comprising:

associating a user with a virtual private server [virtual machine 320, 322 are running at the user level, see Fig. 3; col. 7, lines 45 – 59], the virtual private server comprising a plurality of actual processes [applications 330, 332, Fig. 3; col. 8, lines 5-20];

intercepting a call to the operating system for which actual super-user privileges are required, the call made by a process located in the computer system, the process owned by the user [API is normally a layer of software that defines the set of services offered by the HOS to user-level applications. On operating systems that provide protection, API system calls are implemented by a secure mechanism that allows transitions of the processor between user-level mode and system-level mode; col. 9, lines 29-40]; and

in response to the intercepted call to the operating system pertaining to the virtual private server associated with the user [VMM 360 then sets all parameters required for the I/O request and initiates the request by passing it via the driver 390 (path B) to the user-level device emulator 300; col. 16, lines 20-27]:

granting actual super-user privileges to the user [device emulator 300 then uses the API 392 offered by the HOS 340 to emulate the I/O request; col. 16, lines 27-36]; and

allowing execution of the system call [a privileged instruction emulation module 512 emulates the privileged instructions issued by the virtual machine 320 (FIG. 3) in a safe manner; col. 13, lines 23-33]. Bugnion does not specifically disclose designating a user as a virtual super-user and granting actual super-user privileges to the user.

However, Schneider teaches a virtual private network (VPN) 201 [col. 8, lines 22-50] designating a user as a virtual super-user [administrative policy 305 defines rights of user groups to define/delete/modify objects in VPN 201; col. 10, lines 40-47], intercepting a call to the operating system for which actual super-user privileges are

required [access filter 203 is thus able to control access by the user to the resource by interceding in the communication between a user and a service on the server which is able to provide the user with access to the information resource; col. 16, lines 15-36], granting actual super-user privileges to the user [Access filters 203 are designed such that the decision whether to grant a user access to an information resource need only be made in one of the access filters 203; col. 16, lines 33-50] and allowing execution of the system call [If the access is permitted, the message is once again encrypted and sent to access filter 403(5) nearest server 407; col. 17, line 37-col. 18, line 5].

7. It would have been obvious to a person of ordinary skill in the art at the time of the invention to apply the teaching of designating a user as a virtual super-user and granting actual super-user privileges to the user as taught by Schneider to the invention of Bugnion because this provides scalable and decentralized administration of access to a virtual private network [col. 5, line 60-col. 6, line 7 of Schneider].

8. As to claim 2, Bugnion teaches withdrawing the actual super-user privileges from the user after execution of the call to the operating system [col. 16, line 62 - col. 17, line 5].

9. As to claim 3, Bugnion as modified teaches assigning a virtual super-user identifier to the user [col. 9, lines 39-50 of Schneider].

10. As to claim 4, Bugnion as modified teaches the virtual super-user identifier comprises a super-user identifier and an indication of the virtual private server [col. 9, lines 39-50 of Schneider].

11. As to claim 5, Bugnion as modified teaches assigning a user identifier to the user and storing the user identifier and an indication of the virtual private server of the user in a virtual super-user list [database 301; col. 10, lines 19-48 of Schneider].

12. As to claim 6, Bugnion as modified teaches assigning a super-user identifier to the user [col. 9, lines 39-50 of Schneider].

13. As to claim 7, Bugnion teaches the intercepted call to the operating system comprises a call to the operating system for accessing a file [When the physical device 380 completes its operation, for example, retrieving a requested portion of a file; col. 16, lines 36-62].

14. As to claim 8, Bugnion as modified teaches the intercepted call to the operating system pertains to the virtual private server associated with the user when the file to be accessed is associated with the virtual private server [col. 26, lines 19-28 of Schneider].

15. As to claim 9, Bugnion teaches the intercepted call to the operating system comprises a call to the operating system for terminating a process [col. 11, lines 30-52].

16. As to claim 10, Bugnion teaches the intercepted call to the operating system pertains to the virtual private server associated with the user when the process to be terminated is associated with the virtual private server [col. 11, lines 30-52].

17. As to claim 11, Bugnion teaches identifying each process associated with the virtual private server, and terminating each identified process [col. 11, lines 30-52].

18. As to claim 12, Bugnion as modified teaches a data structure stores associations between processes and virtual private servers, and identifying each process by its association with the virtual private server in the data structure [database 301; col. 10, lines 19-48 of Schneider].

19. As to claim 16, Bugnion teaches responsive to the intercepted call to the operating system not pertaining to the virtual private server associated with the user, disallowing execution of the call to the operating system [One example of a user API

392 request would be a call from an application whose execution requires a level of privilege not granted to applications running at user level, such as instruction calls that would alter certain important registers used only by the processor for its internal control; col. 9, lines 40-52].

20. As to claim 18, Bugnion teaches allowing comprises: executing the call to the operating system [In order for the system-level VMM 360 to use this ability of the user-level device emulator 300 to issue standard operating system calls, some interface is required; col. 8, line 66 - col. 9, line 8].

21. As to claims 21-32, 36 and 38, these are product claims that correspond to method claims 1-12, 16 and 18; note the rejections to claims 1-12, 16 and 18 above, which also meet these product claims.

22. As to claims 41-52, 56 and 58, these are system claims that correspond to method claims 1-12, 16 and 18; note the rejections to claims 1-12, 16 and 18 above, which also meet these systems claims.

23. **Claims 17, 19, 20, 37, 39, 40 and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bugnion and Schneider further in view of U.S. Patent NO. 6,658,571 to O'Brien [cited in previous office action].**

24. As to claim 17, Bugnion as modified does not teach disallowing execution of a system call for inserting a module into an operating system kernel.

However, O'Brien teaches responsive to the intercepted system call comprising a system call for inserting a module [malicious software] into an operating system kernel, disallowing execution of the system call [each security module 105 "wraps" one or more applications 107 in the sense that applications 107 cannot access computing resources 106 for which they are unauthorized in the event that an application 107 executes malicious software; col. 3, lines 39 – 56].

25. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to disallow the execution of a system call for inserting a module into an operating system kernel as taught by O'Brien to the invention of Bugnion as modified by Schneider because this prevents malicious software from damaging computing resources that user is not normally allowed to access [col. 4, lines 33 – 37 of O'Brien].

26. As to claim 19, Bugnion as modified teaches loading a system call wrapper [Security modules 105 are kernel-loadable modules that make and enforce application-specific or resource-specific policy decisions for applications 107; col. 3, lines 38 – 56 of O'Brien], saving a pointer to the system call [each entry includes the following fields: a pointer to the original system call handler within the operating system; col. 5, lines 27 – 46 of O'Brien] and replacing the pointer to the system call with a pointer to the system call wrapper, such that the system call wrapper is executed when the system call is invoked [for each system call being wrapped, security master 103 redirects each pointer from the standard handler within the operating system to a corresponding system call wrapper within security master 103; col. 5, lines 27 – 46 of O'Brien].

27. As to claim 20, Bugnion as modified teaches the pointer to the first system call comprises a system call vector [Conventional operating systems include a system call table (ST) that contains pointers to handlers for the various system calls; col. 5, lines 28 – 46 of O'Brien].

28. As to claims 39 and 40, they are similar in scope to claims 19 and 20; therefore, claims 39 and 40 are rejected for the same reasons as claims 19 and 20 above.

29. As to claims 37 and 57, they are similar in scope to claim 17; therefore, claims 37 and 57 are rejected for the same reasons as claim 17 above.

CONTACT INFORMATION

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Li B. Zhen whose telephone number is (571) 272-3768. The examiner can normally be reached on Mon - Fri, 8:30am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Thomson can be reached on 571-272-3718. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Li B. Zhen
Examiner
Art Unit 2194

lbz

WILLIAM THOMSON
SUPERVISORY PATENT EXAMINER